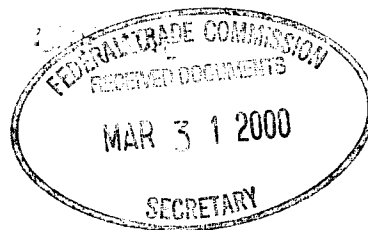




## Securities Industry Association

1401 Eye Street, NW, Washington, DC 20005-2225, (202) 296-9410, Fax (202) 296-9775  
info@sia.com, <http://www.sia.com>

March 31, 2000



Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Rule, 16 CFR Part 313--Comment

Dear Sir or Madam:

The Securities Industry Association ("SIA")<sup>1</sup> appreciates the opportunity to comment on the proposed rules issued by your agency to implement the financial provisions of the Gramm-Leach-Bliley Act ("GLB Act"). SIA supported the enactment of the GLB Act and we commend the effort to draft rules that are consistent with the goals of the legislation's privacy provisions. Although protecting the privacy of customer financial information has always been of utmost importance to the securities industry, we believe that the GLB Act and the implementing regulations provide extensive protections to customer financial information. SIA has filed a detailed letter commenting on the proposed privacy rule issued by the Securities and Exchange Commission, the primary regulator for our member firms, which include, investment banks, broker dealers and mutual fund companies. A copy of that letter is enclosed herewith.

The purpose of this letter is to highlight concerns of our member firms that are common to all of the privacy regulations issued by the regulatory agencies under the GLB Act. We believe this is important because many of our member firms are now or may become affiliated with institutions subject to your regulations and because the regulatory agencies are required to issue final regulations that are "consistent and

---

<sup>1</sup> The Securities Industry Association brings together the shared interests of more than 740 securities firms throughout North America to accomplish common goals. SIA member firms (including investment banks, broker-dealers, and mutual fund companies) are active in U.S. and foreign markets and in all phases of corporate and public finance. The U.S. securities industry manages the accounts of more than 50-million investors directly and tens of millions of investors indirectly through corporate, thrift and pension plans. The industry generates more than \$300 billion of revenues yearly in the U.S. economy and employs more than 600,000 individuals. (More information about SIA is available at our Internet web site, <http://www.sia.com>.)

comparable.” We hope you will consider these comments when drafting your agency’s final rule.

◆ **Flexibility in Compliance**

The rule should allow financial institutions the most flexibility in structuring their compliance efforts. Allowing for such flexibility in the rule’s requirements is critical because financial institutions are varied in their kinds and size of operations, personnel, customer base and types of services and products offered. Rapidly advancing technology, which is changing the way financial services firms to do business at an ever-expanding clip, also dictates that the rule’s requirements be flexible in order to allow institutions to adapt. For these reasons, the rule should allow institutions the utmost flexibility to adopt procedures most suited to their business.

◆ **Consistency Across Industries**

The final rules adopted by each agency should be harmonized with those adopted by the other agencies. This is required by the GLB Act, which provides that to the extent possible “the regulations prescribed by each [] agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities.” SIA urges the regulatory agencies to coordinate their efforts in drafting final rules. In order to achieve the intent of the GLB Act -- affiliations of securities, banking and insurance firms -- the regulations must be applied consistently and evenly across the financial services industries. Differing approaches and regulations by the various agencies will be burdensome and costly for the industry, confusing for consumers, and act as a disincentive for institutions to form the affiliations contemplated by the GLB Act.

◆ **Workable Definition of Nonpublic Personal Information ( §\_\_.3 (n) and (o) )**

With regard to the definition of “nonpublic personal information,” we urge the adoption of Alternative B. The Alternative A definition is unworkable because it would require financial institutions to maintain records of the source from which publicly available information was initially obtained. Clearly, the source from which a financial institution obtained information should not matter if that information is publicly available. Such an approach has no ill effects because consumers should have no expectation of privacy for information that is publicly available.

In addition, SIA believes that the rule’s definition of “personally identifiable financial information” goes far beyond Congress’ mandate to protect *financial* information relating to the consumer. The rule encompasses virtually all personally identifiable information in the possession of a financial institution. The proposal (§\_\_.3(o)(1)) defines nonpublic personal information to include “personally identifiable financial information,” which in turn is defined to include “*any information* (i) provided

by a consumer to [the financial institution] to obtain a financial product or service from [the financial institution]; (ii) about a consumer resulting from any transaction involving a financial product or service between [the financial institution] and a consumer; or (iii) [the financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that customer.” We recommend that the rule be amended to clarify, consistent with Congressional intent, that not all information relating to a customer within the possession of a financial institution would necessarily fall within the scope of the rule.

SIA also suggests that the definition of “personally identifiable financial information” should expressly provide that only “personally identifiable” financial information obtained by a financial institution about a consumer would fall within the definition. This would exclude from the definition of nonpublic personal information aggregated information and other data that do not contain any indicators of personal identity. We recognize the privacy concerns relating to information, such as lists, descriptions or groupings of consumers that is derived from personally identifiable financial information if such aggregated information identifies consumers by name or other specific identifier (such as street addresses or telephone numbers). However, such privacy concerns do not exist for aggregated information that does not contain any identifying information. Clearly, Congress did not intend the G-L-B Act to protect aggregated or other “blind” information that could not be identified with particular consumers or customers.

◆ **Flexibility in the Timing of Privacy Notices ( §\_\_.4 and \_\_.5 )**

The proposed rule requires a financial institution to provide the initial disclosure notice to a consumer “prior to” the time the consumer establishes a customer relationship with the financial institution. As written the requirement will be extremely burdensome, impractical, and confusing for consumers, who will likely receive multiple notices from financial institutions. Moreover, this provision is contrary to the GLB Act, which requires that a financial institution must provide the initial notice “at the time” of establishing a customer relationship. SIA, therefore, recommends that the rule allow for notice to be provided at the same time as other disclosures that are furnished to new accountholders.

We also suggest that the rule clarify that affiliated institutions be permitted to prepare a joint privacy notice when a consumer enters into a customer relationship with any one of the affiliated institutions. In such circumstances, the other affiliated institutions should not be required to deliver the notice again to the customer if the customer enters into subsequent relationships with that institution, as long as the previously provided notice includes the necessary information required for the new customer relationship.

Furthermore, we recommend that the rule permit annual notices to be provided to customers at least once during each calendar year in which the relationship continues rather than during each 12-month period. This will allow institutions, which typically send their annual notices to customers at one time each year, the most flexibility in satisfying the GLB Act's requirement.

◆ **Content of Notices Be Limited to Categories of Information ( §\_\_.6 )**

SIA is concerned that the proposed rule and the accompanying examples may be interpreted in a way that would convert a requirement to disclose general classes of information collected and shared and categories of affiliates or third parties into a requirement to disclose far more detailed information (e.g., the sources of information collected, the lines of business engaged in by entities to whom information is disclosed, and illustrative examples of the information collected from each source). As a result, even the disclosure of a readily understood category (such as information from the customer's own "application") might be interpreted as inadequate unless accompanied by examples (such as "name, address and Social Security number"). Financial institutions should be permitted to use broad-based descriptions of the categories of non-public information disclosed and categories of institutions to which such information may be disclosed. Furthermore, the more detailed the categories are, the less likely large financial institutions will be able to provide one consistent and clear disclosure to customers. Consequently, customers would receive multiple and partly redundant disclosures. In fact, an overly detailed privacy notice may actually be counterproductive to the privacy interest of customers and consumers because they will be less likely to read numerous lengthy and detailed statements of privacy policies received from multiple financial institutions.

◆ **Control Over Method of Opt-Out ( §\_\_.8 )**

SIA requests that the proposed rule be revised to reflect that a financial institution may determine the procedures its customers and consumers may use to opt out of information sharing, and that an institution would not be obligated to process an opt-out request that does not conform to its procedures (e.g., a list of names collected by a third party that does not include account numbers or other identifiers needed by the firm to process the request). We also suggest that the regulations provide that opt-out notices should only be effective if given directly to the institution by the consumer or customer.

◆ **Grandfathering of Existing Joint Marketing and Service Agreements ( §\_\_.9 )**

SIA also suggests that all joint marketing and servicing agreements executed between financial institutions and their vendors as of November 12, 1999 be grandfathered. Many institutions currently have agreements in place that require their contracting partner service providers or joint marketers generally to ensure the confidentiality of customer information provided under the agreement. Unless existing agreements are grandfathered, institutions would be required to conduct detailed reviews

of all service provider or joint marketing agreements currently in force (and expired agreements, to the extent that vendors may still possess the firm's customer information) to ensure that the agreements require the vendor to treat the consumer information according to the financial institution's standards. However, the cost of such a review would exceed any relative benefit that could be obtained. Therefore, the rule should not apply retroactively, and existing agreements would be grandfathered. Alternatively, the rule should establish by example that institutions may comply with respect to existing contractual relationships by sending a notice to all vendors informing them of the G-L-B Act and the rule's requirements, and clearly establishing that the agreement and performance thereunder are governed by such requirements.

◆ **Clarify When Disclosure of Account Numbers is Permissible ( §\_\_.13 )**

SIA requests that the rule clarify that the prohibition under rule §\_\_.13 applies only to disclosing account numbers and passwords to nonaffiliated third parties who are not subject to one of the exceptions under rules §\_\_.9, §\_\_.10, and §\_\_.11. While SIA recognizes the sensitivity of customer account numbers and passwords, we nevertheless believe that the rule should include a limited exception for disclosure with customer consent even when the nonaffiliated third party does not fall within rules §\_\_.9, §\_\_.10, and §\_\_.11. Comment was invited on whether the proposed rule should permit the disclosure of encrypted account numbers if the financial institution does not provide the marketer the key to decrypt the number. The SIA urges that the rule be revised to specifically permit the sharing of encrypted or truncated numbers.

◆ **Reconsider The Effective Date**

We strongly urge that the effective date be extended, as agencies are authorized to do under the GLB Act, at least until May 14, 2001. This is vital in order to provide an orderly transition and to allow financial institutions the necessary time to implement firm wide operational changes throughout all of their systems. SIA believes that an effective date of November 13, 2000, would result in the mailing of millions of notices to consumers in December, the peak of the holiday season, which would be ill-timed for consumers, financial institutions and the U.S. mail system. Indeed, consumers may not be able to focus on these notices in the midst of the holiday mail deluge.

We respectfully suggest that the November date be considered as the beginning of a voluntary compliance period that would end on May 14, 2001, when mandatory compliance would begin. The establishment of a voluntary compliance period would enable financial institutions to use first quarter account statement mailers as a means to satisfy the initial notice requirement. In light of the regulatory and consumer focus on privacy issues, we believe that as a competitive matter, firms will have an incentive to comply fully with the regulation as early as possible.

Additional time is crucial to enable institutions to fully implement operational changes necessary to comply with obligations. All financial institutions will need to (1)

March 31, 2000

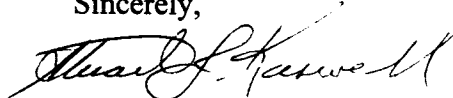
Page 6

establish and implement new procedures and train associates with regard to the delivery of the notice and customer questions that may ensue; (2) implement new procedures for providing opt-out methods to the customers; (3) hire and train staff for receiving and handling any opt-outs from customers; and (4) evaluate arrangements with nonaffiliated third parties to determine what additional obligations must be imposed. Only after all these procedures have been addressed, will firms have sufficient information to request computer system enhancements, which will take significant lead time, resources and money to implement. Moreover, completing these changes in a hasty manner, given the broad scope of the changes, will likely result in mistakes or confusion on the part of the firm, associates and customers alike.

### **Conclusion**

SIA applauds the regulatory agencies for proposing rules that attempt to balance the privacy needs of consumers with the regulatory burdens imposed on financial institutions. We hope that our comments are helpful. If we can provide any further information, please contact Alan Sorcher, Assistant Vice President and Assistant General Counsel at (202) 296-9410.

Sincerely,

A handwritten signature in dark ink, appearing to read "Stuart J. Kaswell", written in a cursive style.

Stuart J. Kaswell

Senior Vice President and General Counsel

Enclosure



## Securities Industry Association

---

1401 Eye Street, NW, Washington, DC 20005-2225, (202) 296-9410, Fax (202) 296-9775  
info@sia.com, <http://www.sia.com>

March 31, 2000

Mr. Jonathan G. Katz  
Secretary  
U.S. Securities and Exchange Commission  
450 Fifth Street, N.W.  
Washington, D.C. 20549-0609

**Re: File No. S7-6-00 (Regulation S-P)**

Dear Mr. Katz:

The Securities Industry Association ("SIA")<sup>1</sup> appreciates the opportunity to comment on the proposed rules issued by the Securities and Exchange Commission ("SEC") that would implement the financial privacy provisions of the Gramm-Leach-Bliley Act ("G-L-B Act"). The G-L-B Act highlights the financial services industry's obligation to respect the privacy of customers and to protect the security and confidentiality of those customers' nonpublic personal information. Accordingly, the Act places certain restrictions on financial institutions regarding the disclosure of consumers' nonpublic personal information to nonaffiliated third parties and requires financial institutions to disclose (i) their privacy policies and practices with respect to the sharing of that information with affiliates and nonaffiliated third parties; and (ii) their procedures for securing their customer's nonpublic personal information.

Among SIA's primary recommendations are that the SEC should: 1) treat examples in the proposed rules as non-exclusive safe harbors; 2) refine the definition of "nonpublic personal information" to include only "financial" information, as intended by the G-L-B Act, and exclude aggregated information and blind data that do not contain personal identifiers; 3) provide additional clarification regarding certain other definitions, including the definitions of

---

<sup>1</sup> The Securities Industry Association ("SIA") brings together the shared interests of nearly 800 securities firms in North America to accomplish common goals. SIA member firms (including investment banks, broker-dealers, and mutual fund companies) are active in U.S. and foreign markets and in all phases of corporate and public finance. The U.S. securities industry manages the accounts of more than 50 million investors directly and tens of millions of investors indirectly through corporate, thrift, and pension plans. The industry generates more than \$300 billion of revenues yearly in the U.S. economy and employs more than 600,000 individuals. More information about SIA is available at our Internet web site, <http://www.sia.com>.

“consumers,” “customers,” and “nonaffiliated third parties;” 4) promote further flexibility in the regulation with respect to the timing of privacy notices to be sent to customers, the level of detail in such notices, and the opt-out procedures; 5) grandfather joint marketing and servicing agreements that were executed before the G-L-B Act became effective; 6) clarify the circumstances under which account numbers may be shared; and 7) reconsider the feasibility of the November effective date. In addition, our letter addresses many other related issues on which the SEC invited comment.

## **I. General Comments**

The SIA applauds the SEC for drafting proposed rules that are generally consistent with the goals and provisions of the G-L-B Act and that seek to avoid placing unnecessary regulatory burdens on the securities industry. The SIA urges the SEC to keep in mind the broad deregulatory intent of the G-L-B Act when implementing and administering the Act’s privacy provisions. In particular, we note that by authorizing affiliations among securities, insurance, and other financial institutions, Congress expressed its intent to remove the artificial and inefficient restrictions that historically have constrained the type of service that financial services institutions can offer their customers. Accordingly, we are encouraged by the flexible approach that the SEC has adopted in various portions of the proposed rules, and we urge the SEC to extend that approach to other portions of the rules, as discussed below.

The SIA also commends the SEC for including examples to clarify the scope and intent of the rules. We believe that such examples promote better understanding and interpretation of the rules, and we have suggested additional examples below. Given that more and more securities firms and other financial institutions are offering their customers an online channel to do business, we believe as a general matter that more examples in that context would be helpful, and we have included several below.

Furthermore, the SIA respectfully suggests that the SEC treat examples in the proposed rules (see rule 248.2) as non-exclusive safe harbors, so that compliance with examples would constitute compliance with the rules themselves. Not only would such an approach be consistent with that taken by the banking agencies in their proposed rules, it also would give firms clear regulatory guidance on which they can rely. We believe that the examples are sufficiently specific that firms will not interpret them in an unduly broad manner. To the extent that the SEC concludes, however, that a safe harbor approach would be inappropriate, we request that the SEC recognize that conduct in accordance with the examples would establish a strong presumption (that may only be rebutted by specific finding of intent to commit a violation) of compliance with the rules.



## II. Scope of the Proposed Rule -- Definitional Issues

### A. Nonpublic Personal Information and Personally Identifiable Financial Information - Rules 248.3(t) and (v)

Under the G-L-B Act, a financial institution must provide its customers with a notice of its privacy policies and practices and generally must not disclose nonpublic personal information about a consumer to nonaffiliated third parties unless the institution has provided the consumer with notice and an opportunity to opt-out of the disclosure. The G-L-B Act defines "nonpublic personal information" as "personally, identifiable *financial* information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."<sup>2</sup> During the Senate's consideration of this section, Senator Gramm clarified at Senator Allard's request that it was his understanding "that the term 'nonpublic personal information' as that term is defined in section 509(4) of title V, subtitle A, applies to information that *describes an individual's financial condition* obtained from one of the three sources as set forth in the definition."<sup>3</sup>

In its current rule proposal, however, the SEC has construed this definition to encompass virtually all personally identifiable information in the possession of a securities firm. The proposal defines nonpublic personal information to include "personally identifiable financial information," which in turn is defined to include "*any information* (i) provided by a consumer to [the firm] to obtain a financial product or service from [the firm]; (ii) about a consumer resulting from any transaction involving a financial product or service between [the firm] and a consumer; or (iii) [the firm] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that customer." Rule 248.3(v). The SIA believes that this definition goes far beyond Congress' mandate to protect *financial* information relating to the consumer. We therefore respectfully recommend that the rule be amended and additional examples be included to clarify that not all information relating to a consumer within the possession of a firm would necessarily fall within the scope of the rule.

The SIA also suggests that the definition of "personally identifiable financial information" expressly state that only *personally identifiable* financial information obtained by a firm about a consumer would fall within the definition. The SIA strongly believes that aggregated information and other data that does not contain any indicators of personal identity should be *explicitly excluded* from the definition of nonpublic personal information. While we understand the privacy concerns relating to lists, descriptions or groupings of consumers derived from personally identifiable financial information if such aggregated information identifies consumers by name or other specific identifier (such as specific street addresses or individual

---

<sup>2</sup> Gramm-Leach-Bliley Act Section 509(4), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (emphasis added).

<sup>3</sup> 145 Cong. Rec. S13902 (daily ed. Nov. 4, 1999) (colloquy between Sen. Allard and Sen. Gramm) (emphasis added).

telephone numbers), we simply do not believe that Congress intended the G-L-B Act to protect aggregated or other “blind” information that does not include such identifiers. For example, data aggregated by zip code or area code would not divulge personally identifiable information regarding any particular consumer or customer with that zip code or area code.

The use of data that cannot be linked to any individual customer or consumer does not implicate the privacy concerns of such customer or consumer. At the same time, this aggregated data is very important to firms, which frequently analyze aggregated data for trends and patterns. Securities firms often define themselves and advertise on the basis of aggregate customer information, such as number and type of accounts, total assets in clients’ accounts under management, and profiles of their customer base. In some instances, they may share such analysis or aggregated data, which have no personal identifiers, with third parties for market analysis or research to improve the firm’s products. Such analysis and research enables the firm to understand its own customers better and to provide better services. Firms may also provide aggregated information regarding its customers to research companies that follow and track the securities industry. This enables such companies to compile trend and analysis reports that are typically made available to the public. Firms may also provide aggregated information, such as a list of the 20 stocks most frequently purchased by its customers, to newspapers, other publications or academics. Although this information is obtained from the securities firm and relates to the firm’s customers, it is not personally identifiable; therefore, we do not believe that this is the sort of information Congress intended to protect under the G-L-B Act or its regulations. To permit individual customers to opt-out of the sharing of aggregated personally identifiable financial information that does not contain personal identifiers would undermine the integrity and reliability of such aggregated information and hamper the ability of firms to provide better customer services. Yet such a rule would do nothing to further individuals’ privacy interests.

Finally, the SIA questions the practicality of the example in rule 248.3(v)(2)(i)(D) which provides that “other information about your consumer if it is disclosed in a manner that indicates the individual is or has been your *consumer*” constitutes personally identifiable financial information. In light of the broad definition of “consumer,” it is difficult to imagine how a firm could disclose information in its possession about an individual without at least suggesting that the firm might have such information because the individual is or has been at some point a consumer (as opposed to a customer) of the firm. We would also note that this example is inconsistent with rule 248.3(t)(2)(i) which states that nonpublic personal information does not include publicly available information except when the information “is disclosed in a manner that indicates the individual is or has been your *customer*” and with rule 248.3(t)(2)(ii) which provides that nonpublic personal information does not include “any list, description or other grouping of *consumers* (and publicly available information about them) that is derived without using any personally identifiable financial information.”

B. Publicly Available Information - Rule 248.3(w)

The SIA commends the SEC for endorsing the proposed definition of “publicly available information.” We believe that the alternative definition is overly broad and burdensome because it would require firms to maintain records of the source from which publicly available information was initially obtained. If information is publicly available, the source from which a firm obtained that information should be irrelevant. Similarly, we believe that all information that is disclosed or required to be disclosed by operation of law, whether it be foreign or domestic law, should be considered publicly available.

We also request that the examples of information from “widely distributed media” be modified. The proposed examples currently include information from “an Internet site that is available to the general public without requiring a password or similar restriction.” We believe that widely distributed media should include Internet sites that may require some form of registration and/or password as long as the requirements for registering or obtaining a password are comparable to the requirements for obtaining a subscription to a newspaper or other such media. For example, certain newspaper web sites (such as the New York Times site) require individuals to register and create a password to access its content even though the newspaper itself would generally be considered “widely distributed media.”

C. Consumers - Rule 248.3(g)

The proposed rule defines a “consumer” as an individual who obtains from a firm financial products or services primarily for personal, family, or household purposes. Examples of “consumers” in the proposal appropriately identify instances in which an individual is or is not a consumer. The SIA suggests that the SEC include additional examples to clarify that an “individual” includes only natural persons. In particular, we request that the SEC expressly recognize that entities such as partnerships, trusts, and personal holding companies are not consumers under the proposed rule, because they are not individuals. We also believe that 401(k) plan participants would not qualify as “consumers” of the securities firm affiliates that act as 401(k) plan trustees or record keepers. In that situation, the 401(k) plan administrator would be the consumer or customer of the firm, not the employees who participate in the 401(k) plan. To the extent that the qualified plan trustee (or employer) who is the primary account holder is not an individual, we believe it would be helpful for the SEC to clarify that it would not be a “consumer” or “customer” under these rules.

The proposed definition of “consumer” also includes an individual’s “legal representative.” The SIA requests additional clarification of the term “legal representative” and a firm’s obligations towards an individual who has a legal representative. In particular, the SIA believes that a firm should be able to fulfill its obligations under this regulation towards an individual who has a legal representative (such as a minor who is represented by a custodian) by

providing the appropriate notice and opt-out opportunity to the legal representative.<sup>4</sup> In some instances, a legal representative may not even provide the firm with information about the beneficiaries. As we discuss below, requiring firms to provide notices to these unknown beneficiaries would be illogical at best.

The SIA appreciates the guidance provided by the examples to the definition of “consumer.” We would suggest that example (ii) be clarified to include situations in which the individual does not open an account or place an order but provides basic information on a web site form to participate in an online seminar or forum, to use basic informational or educational tools on a web site, to view or access a web site, or to request general information and updates about products, the market, or the securities firm. We also request that the SEC include an example involving omnibus and other accounts that are opened by registered investment advisers, banks or other intermediaries without disclosing to the securities firm the identity of the underlying customers or beneficiaries. When a firm does not know the identity of an underlying account holder, we submit that the underlying account holder should not be deemed the firm’s “consumer” or “customer” and that the firm should have no obligation to that person under these rules. This approach is consistent with other examples in the proposed rules which provide that undisclosed customers who have interests in securities in broker-dealer omnibus accounts or mutual fund shares held in street name are not consumers of such broker-dealer or mutual fund. It is also consistent with the SEC’s position that a fully disclosed clearing arrangement creates a customer relationship between the clearing firm and the introducing firm’s customer.

Finally, we request additional guidance regarding the obligations of securities firms when an employee leaves one firm and goes to another. We believe that consumers or customers of the prior employer would not constitute consumers of the new employer until and unless they obtain or seek to obtain a financial product or service from the new employer, and such persons would not constitute customers until such time that they establish a customer relationship with the new employer. With respect to the prior employer, while we believe that the G-L-B Act requires firms to establish and maintain reasonable policies and procedures to safeguard personally identifiable financial information about consumers and customers, we do not believe that it requires a firm to be a guarantor against the possibility that an employee may take such information in violation of those policies and procedures. Accordingly, we request that the SEC clarify that a firm will not face any liability for disclosures of personally identifiable financial information resulting from the independent acts of a firm’s former employee that violate any contractual or other duty owed to the firm.

---

<sup>4</sup> The SIA also requests confirmation that the inclusion of “legal representative” in the definition of “consumer” is not intended to suggest that the legal representative, in his or her own capacity, becomes the financial institution’s “consumer” simply by virtue of his or her representation of a beneficiary who is a consumer.

D. Customers - Rule 248.3(j)

The SIA applauds the SEC for providing helpful guidance establishing that a single isolated transaction in most circumstances does not establish a customer relationship. We suggest that this example should not be limited to a single transaction because some individuals may conduct a *de minimis* number of sporadic, infrequent transactions and not be a customer of the firm.

We encourage the SEC to include additional examples illustrating when a consumer is or is not a customer of a securities firm. For example, if an individual purchases shares of a mutual fund from a broker-dealer and the mutual fund complex carries the customer's securities in the customer's name and future transactions between the customer and the mutual fund complex occur directly without the involvement of the broker-dealer, the individual should not be treated as a customer of the broker-dealer. That is because the broker-dealer only acted as the initial sales conduit for the mutual fund and does not independently have a continuing obligation with the consumer. (On the other hand, if the primary relationship is between the broker-dealer and the individual, the customer relationship would be between the individual and the broker-dealer, not the mutual fund complex.) Similarly, if a broker-dealer sells a life insurance product to an individual and an unaffiliated insurance company underwrote the product, the individual should not be deemed a customer of the broker-dealer based on that single transaction. In both of these examples, the broker-dealer's sole role was to introduce the consumer to the mutual fund complex or insurance company, at which point the broker had no continuing role in the ensuing relationship. In sum, we believe that only the institution with the ongoing customer relationship should be required to provide the notices required under this rule.

Finally, we note that the initial privacy notice requirement for customers is inconsistent with one of the examples under the definition of "customer." The example provides that effecting a single securities trade for a consumer on an accommodation basis would not make the consumer a customer of the firm. The initial notice requirement at rule 248.4(c)(2)(i), however, provides that a customer relationship exists when a particular consumer "effects a securities transaction." We suggest that the SEC amend the definition of customer in the initial notice example to encompass only consumers who "regularly effect securities transactions."

E. Clear and Conspicuous - Rule 248.3(c)

Although the SIA appreciates the importance of providing notice that is clear and conspicuous, we respectfully submit that the SEC need not define "clear and conspicuous" for purposes of this regulation because the financial industry has already developed certain standards of "clear and conspicuous" in connection with existing practices and regulations, including many of the banking regulations, such as Regulations D, E and Z of the Federal Reserve Board. The proposed definition, which differs from existing terminology under "clear and conspicuous" would lead to uncertainty and confusion in compliance and legal standards. We are also concerned that the examples provided in rule 248.3(c) may appear to establish rigid requirements

that take away flexibility that a firm might have in drafting notices that comply with the regulation.

F. Control - Rule 248.3(i)

The definition of “control,” which defines when an entity is an “affiliate,” adds to an already complex array of definitions of control and affiliate in the federal securities laws and the regulations of the self-regulatory organizations. To streamline and avoid any unnecessary ambiguity, we suggest that the SEC adopt the definition of “control” that is used in Form BD to determine when an entity is a “control affiliate” for purposes of this regulation.<sup>5</sup> The Form B-D definition is substantially similar, but not identical, to the definition proposed in rule 248.3(i).

G. Financial Institution – Rule 248.3(m)

The proposed definition of “financial institution” could be read to include independent contractor registered representatives of a broker-dealer. We recommend that the SEC clarify that such independent contractors are not separate “financial institutions” under the terms of the rule when acting in the capacity of a registered representative of a broker-dealer. This would be consistent with treatment of both employee and independent contractor registered representatives of a broker-dealer as associated persons of the broker-dealers under the Securities Exchange Act of 1934. This approach provides the same protections to customer nonpublic personal information because the broker-dealer is obligated to supervise the conduct of such representatives and all other associated persons, including the duty to ensure customer information is used only as allowed by the broker-dealer and in compliance with the proposed rule and other applicable laws. The same concept would extend to individual independent contractors who are associated persons of an investment adviser under the Investment Advisers Act of 1940. We strongly encourage the SEC to clarify that registered representatives and other associated persons of a broker-dealer and associated persons of an investment adviser are not separate financial institutions and do not have notice or other requirements other than those the financial institution imposes and is required by the rules to perform. Under the various notice requirements, the registered representatives, other associated persons and any employee of a financial institution should be deemed to be acting on behalf of the financial institution and no separate compliance requirements should be imposed upon them.

H. Nonaffiliated Third Party - Rule 248.3(s)

As the SEC is aware, the federal securities laws and the rules of the self-regulatory organizations permit firms to have associated persons who are independent contractors and not employees of the firm. The SIA is concerned that the definition of “nonaffiliated third party” is so broad that such independent contractors could be deemed to be nonaffiliated third parties. We

---

<sup>5</sup> In making this suggestion, the SIA does not mean to suggest that the definition of “affiliate” should include *only* those entities that would be “control affiliates” under the Form B-D definition. The SIA endorses the SEC’s proposal to include in the definition of “affiliate” those entities that would be deemed an affiliate under the banking agencies’ proposals.

request that the exceptions provided in rule 248.3(s)(1) be expanded to include independent contractors who are associated persons of a particular securities firm, as well as temporary employees, directors, and other agents of the firm who carry out the business of the firm but may not necessarily fall within the classification of "employee." To the extent that these people are engaged in performing functions for the firm that the firm would otherwise perform directly for itself, they should not be distinguished from the firm's employees. We suggest revising exception (ii) to include "a person acting jointly for you as your employee, agent or independent contractor and any company that is not your affiliate." We also suggest that a third exception be carved out for "a person who is one of your directors, temporary employees, agents or independent contractors."

The SIA requests additional clarification of rule 248.3(s)(2), which provides that nonaffiliated third parties include a company that is an affiliate by virtue of merchant banking or investment banking activities. In particular, we respectfully submit that to the extent a securities firm establishes a venture capital or other partnership or fund to engage in merchant banking or investment banking activities, that partnership or fund would be an affiliate of the firm.

### **III. Initial and Annual Notice - Rules 248.4, 248.5 and 248.6**

The G-L-B Act requires a financial institution to provide a notice of its privacy policy to customers and consumers. For customers, the notice must be provided at the time of establishing the customer relationship, and at least annually thereafter. For consumers who are not customers, the notice must be provided before disclosing nonpublic personal information.

#### **A. Timing - Rule 248.4(a)**

The proposed rule requires a securities firm to provide the initial notice prior to the time that the firm establishes a customer relationship with the consumer. The SIA requests that the SEC allow the notice to be provided at the same time as other disclosures (such as margin and credit disclosures) that are furnished to new accountholders, and not mandate an earlier disclosure that could require a separate mailing. As the SEC acknowledged in the proposing release, there is an interest in "striking" a balance between (i) ensuring that consumers will receive privacy notices at a meaningful point when 'establishing a customer relationship' and (ii) minimizing unnecessary burdens on financial institutions that may result if a financial institution is required to provide a consumer with a series of notices at different times in a transaction." Preamble to proposed rule 248.4(a), 65 Fed. Reg. 12354, 12,359 (2000). The rule therefore contemplates that the privacy notice may be given at the same time as other notices.

The SIA believes that the proposed requirement that notice be provided *prior* to the establishment of a customer relationship is inconsistent with the language of the G-L-B Act, which requires that disclosure be made "at the time of establishing a customer relationship." 15 U.S.C. 6803(a). Moreover, furnishing the notice prior to the establishment of a customer relationship may simply not be practicable in certain circumstances. For example, after an introducing broker establishes a new customer relationship for itself, and subsequently for its clearing broker, the clearing broker mails a "382 Notice" to the new customer. Including the

privacy notice with or as part of the 382 Notice should be sufficient, even though it is not and could not be mailed out before the clearing broker becomes aware of the existence of the new customer relationship. In addition, for customer relationships established over the telephone, we believe that it is unnecessary and cumbersome to require firms during the telephone call to obtain the customer's oral agreement to receive the privacy notice subsequently in writing. In any event, under the G-L-B Act and the proposed rules, securities firms may not share a customer's information with nonaffiliated third parties until after the customer has received a privacy notice and has been given a reasonable opportunity to opt-out.

As a general matter, we urge the SEC to give firms the flexibility to deliver the initial notice within a reasonable period after the customer relationship is established, provided that no nonpublic personal information relating to the customer is disclosed to a nonaffiliated third party before the initial privacy and opt-out notice and a reasonable opt-out period have been provided. Providing a privacy notice in this manner gives the customer the opportunity to opt-out well in advance of the time any privacy rights might be threatened. Firms could also make their privacy policies generally available in branch offices, on their web sites, or upon request by phone, so consumers who want to compare privacy policies before applying would be able to do so without making the privacy notices a mandatory part of the application process itself.

We also request that the SEC clarify that affiliated institutions be permitted to prepare a joint privacy notice to be delivered when a consumer enters into a customer relationship with any one of the affiliated institutions. In such circumstances, the other affiliated institution(s) would not need to deliver the notice again to the customer if the customer enters into a subsequent relationship with that institution, as long as the previously provided notice included the necessary information required for the new customer relationship.

**B. Manner- Rule 248.4(d)**

The SIA requests that the SEC clarify that when a prospective customer submits an electronic application through a web site, the burdens for electronic delivery of the required privacy notice should be no greater than paper delivery of the notices. Provided that a firm makes its privacy notice always available on its web site and that its online application process includes a prominently displayed link to the firm's privacy notice, we believe there should be no requirement that a customer must click-through the entire notice or that the firm record the fact that a customer has clicked-through the notice. Such a requirement would add significantly to the burdens placed on both customers and firms who elect to do business electronically and, at the very least, would need to be addressed in the Cost-Benefit Analysis and Paperwork Reduction Act sections of the proposed rule.

**C. Content - Rule 248.6**

The rule requires that the annual and initial notices that a firm provides to its customers describe, among other things, the categories of (1) nonpublic personal information about consumers that are collected and/or disclosed; and (2) affiliates and nonaffiliated third parties to whom nonpublic personal information is disclosed (other than those expressly permitted under



the rule). We do not believe that the G-L-B Act requires disclosures with regard to sharing of affiliate information and that disclosures regarding affiliate relationships should be limited to the requirements under the Fair Credit Reporting Act.

The SIA is concerned that the proposed rule and the examples accompanying it may be interpreted in a way that would convert a requirement to disclose general classes of information collected/shared and categories of affiliates or third parties into a requirement to disclose far more detailed information (e.g., the sources of information collected, the lines of business engaged in by entities to whom information is disclosed, and illustrative examples of the information collected from each source). As a result, the disclosure of even a readily understood category (such as information from the customer's own "application") might be interpreted as inadequate unless accompanied by examples (such as "name, address and Social Security number"). The SIA requests that the SEC clarify that these examples are not meant to expand the statutory requirements of the G-L-B Act.

Information that a firm "collects" is defined in the proposed rules to include any data that is "retrievable on a personally identifiable basis." See rule 248.3(d). We request that the SEC clarify the intended scope of the definition, with respect both to paper-based information and to electronically stored information. In particular, we request that the SEC make clear that in the context of electronic databases, this definition only covers that information that is retrievable in the database by name, social security number, account number, or other personal identifier. At a minimum, we urge the SEC to change the proposed definition to "easily accessible" or "practicably retrievable" by the firm. The current proposal would cover, for example, notes about a client kept in a stockbroker's "personal" file (a Rolodex, for example). Though this information is not maintained in the firm's database, and the firm may not even know of its existence, it is theoretically "retrievable" by the firm. Similarly, under the proposed definition, a firm may be considered to "collect" the identity of payees of checks and share drafts that are written by its customers. While such information may not be maintained in readily accessible format, and is rarely if ever disclosed to third parties, it too is theoretically "retrievable." Thus, the proposed definition may have the unintended consequence of requiring securities firms to disclose that they "collect" payee information. Therefore, the SIA respectfully suggests that the SEC limit this definition to information that securities firms maintain in an easily accessible format and collected with the intention of disclosing to third parties.

We further suggest that the SEC permit firms to use broad-based descriptions of the categories of nonpublic personal information disclosed and categories of institutions to which such information may be disclosed. The more detailed the categories are, the less likely large financial institutions will be able to provide one consistent and clear disclosure to customers and associates who answer customer questions. An overly detailed privacy notice may actually be counterproductive to the privacy interest of customers and consumers because they will be less likely to read numerous lengthy and detailed statements of privacy policies received from multiple financial institutions. Additionally, if the level of detail required is so intricate, many firms would be precluded from using one disclosure for an institution as a whole; consequently, customers would receive multiple partly redundant disclosures.

Some firms may choose not to disclose information to nonaffiliated third parties that fall outside the scope of one of the enumerated exceptions to the opt-out provisions. For these firms, the SIA requests that rule 248.6(d)(4) – “simplified notices” – make clear that the required privacy notice need not include an explanation of the opt-out right (nor must an opt-out notice be given) otherwise required under rule 248.6(a)(6) or identify the categories of information collected.

D. Annual Notices - Rule 248.5

The SIA requests that the SEC amend the proposal so that the standard for defining when a customer is active or inactive is based upon the firm’s definition of an inactive account for other regulatory purposes. This is consistent with several banking regulations that recognize that a financial institution need not provide periodic statements to consumers whose accounts become inactive as defined by the institution. See 12 C.F.R. 205.9(b)-3. Requiring the annual notice to continue to be delivered on accounts for 5 to 10 years after activity ceases places an unnecessary cost and burden on the firm without any benefit to the customer. In such instances, the account may be in a holding period between activity and being escheated to the state.

The SIA also requests that the SEC revise the definition of “annually” to permit firms to provide notices at least once per calendar year. As a matter of logistics and practicality, firms are simply unable to send annual notices to customers on the basis of each account’s anniversary date. Permitting firms to rely on a calendar year to determine annual notice dates will give firms much needed flexibility without noticeably decreasing the protection given to customers.

E. Opt-Out - Rules 248.7 and 248.8

The G-L-B Act generally prohibits a financial institution from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution gives the consumer notice of the institution’s privacy policy and practices -- including a clear and conspicuous notice that the consumer’s information may be disclosed to unaffiliated third parties -- and gives the consumer the opportunity to opt out of such sharing.

*1. Manner - Rule 248.8(b)*

The proposed rule seems to endorse the use of written opt-out responses from consumers, as well as the use of electronic means “if the consumer agrees to the electronic delivery of information.” That provision should be amended to make it unambiguous that a firm may permit electronic opt-outs by e-mail or on the firm’s web site. Furthermore, the SIA requests that the rule include an example clarifying that a customer who is doing business with a firm electronically at the time the firm is providing the required privacy notice may be deemed to have consented to the delivery of the opt-out notice electronically. This would apply when a customer is applying to open an account online.

Although the rule seems to permit electronic opt-outs, it does not authorize telephonic opt-out. Currently, many firms that permit customers to opt-out of information sharing allow customers to do so by telephone. The SIA proposes that the rule give firms the flexibility to decide to permit customers to opt-out telephonically, either by speaking with a firm representative or through an automated telephonic system.

*2. Joint accounts - Rule 248.7*

The SIA requests that the rule establish that providing an opt-out notice to one party on a joint account would be sufficient. We suggest that this notice should be given to the primary accountholder or the person whose social security number appears on the account at the address of record as identified on the firm's records. We submit that the rule should not require that notices be provided to each accountholder. Requiring notice to each accountholder would impose an undue administrative burden because it would require firms to track and record whether each accountholder has opted-out before any nonpublic personal information can be shared. Moreover, as a practical matter, it may be impossible to segment each accountholder's information in joint accounts (e.g., information about household net worth). We further request that the rule be clarified to permit a firm to discharge its responsibility by giving notice to anyone with discretionary authority over the account or a power of attorney so long as that party is not affiliated with the firm.

*3. Timing - Rule 248.7(a)(3)(i)*

The SIA supports the proposed rule's establishment of 30 days as a reasonable time period for a consumer to exercise his or her right to opt-out by mail. The SIA suggests that the SEC should also specify reasonable periods for all of the other links in the opt-out process. Accordingly, a firm should have a reasonable period of time after the proposed rules become effective to deliver notices to customers and consumers. Furthermore, firms should have a reasonable amount of time to implement an individual customer's election to opt-out of information sharing with nonaffiliates.

*4. Joint notices - Rule 248.8(b)(3)*

The SIA endorses the proposed rule's recognition that a privacy notice may be combined with other required notices or with other information generally made available to customers or consumers. Providing the notices in that fashion will facilitate customers' understanding of their rights under the regulation. We submit that enabling firms to include such information would help customers to make fully informed decisions about whether to opt out or not. As we discussed above, the benefits inherent in sending joint notices argue in favor of permitting the privacy notice to be given to a new customer at the same time as other new account opening documents -- and not necessarily prior to the establishment of a customer relationship.

*5. Model opt-out - Rule 248.8*

The G-L-B Act requires that the notices provided to consumers be "clear." The SIA urges the SEC to give firms the flexibility to use language best suited to its needs to provide clear and conspicuous notice. We do not believe it is necessary to have a rule that specifically discourages the use of boilerplate or legal terminology in the consumer opt-out notice. Indeed, we believe that such a provision may be counterproductive and result in more opaque disclosures rather than simpler disclosures. Given the legal and technical issues that may be involved, as well as the commonality of issues faced by all financial institutions, common and/or technical language may be appropriate and may not necessarily bear on whether a particular notice is clear and understandable. By proscribing or discouraging certain types of language, the SEC might unintentionally create unwarranted exposure to enforcement actions or third party rights. Finally, to assist securities firms in adopting clear and consistent opt-out notices, we request that the SEC develop model forms, the use of which would constitute safe harbors under the rule.

*6. Control over method of opt-out - Rule 248.7*

The SIA requests that the SEC amend the proposed rule to provide that a firm may determine the procedures its customers and consumers may use to opt out of information sharing, and that a firm would not be obligated to process a non-conforming opt-out request (e.g., a list of names collected by a third party that does not include account numbers or other identifiers needed by the firm to process the request). We also suggest that the regulations provide that the opt-out notices should only be effective if given directly to the firm by the consumer/customer. We submit that such an approach would not only ease administrative burden on the firm but also be in accord with legislative intent. Section 502 of the G-L-B Act requires that consumers receive "an explanation of how the consumer can exercise [the] nondisclosure option." That language demonstrates a Congressional intent to give firms the authority to determine the method(s) for consumers to exercised their opt-out right. Such a requirement would help guard against disruptions occasioned by the receipt of mass lists compiled by a third party that include both the consumers of the firms' services and thousands of other individuals. For example, a firm might receive an emailed list from a web site operator of individuals (whether customers of the firm or not) who have a general interest in restricting the disclosure of personal information. It would be inconsistent with Congress' intent and unduly burdensome to require a firm to act on such a mass, emailed list. Moreover, requiring direct contact between the individual and the firm may avoid misunderstandings and abuse that may result from the intervention of a third party intermediary.

**IV. Exceptions to Opt-Out Requirement - Rules 248.9, 248.10, 248.11**

The SIA requests that the exception under 248.11(a)(1) permitted for data transfers that are made in accordance with a customer's consent be clarified to permit the consent to be provided orally, and that such consent need not be obtained in writing. If oral consents are not acceptable, consumers may be frustrated by a firm's inability to share information, such as

information about assets held with a mortgage lender, in a timely fashion, and the processing of other financial transactions may be slowed down.

The exception under 248.11(a)(1) appropriately reflects that customers routinely request their broker-dealers to disclose their nonpublic personal information to third parties in many different contexts. We are concerned that the proposed rule may unnecessarily require an additional customer consent in situations where the customer has already authorized the broker-dealer to share information. To provide clearer guidance, SIA suggests that the rule include under this exception examples of situations where the customer has provided consent, as follows:

- A brokerage account application, signed by the customer, includes the customer's standing authorization for the broker-dealer and the customer's investment adviser to share the customer's account and personal information.
- A brokerage account application, or similar form, authorizes the broker-dealer to follow the future instructions of the customer's investment adviser (or other fiduciary) with respect to disclosing the customer's information to nonaffiliated third parties.
- A broker-dealer informs customers that their voluntary participation in a particular program, or in a referral process to a nonaffiliated third party, will require the broker-dealer to share the customer's information with the nonaffiliated third party. When the customer registers, applies, or subscribes to participate in that program or referral process, he or she has consented to that disclosure of information.

In these situations, the rule should not require an additional consent before enabling customers to direct where their information is sent. Such an additional requirement would be inefficient and counter to those customers' interests. In addition, there are other situations in which customers should be deemed to have consented to the "disclosure," such as when consumers register or subscribe for co-branded products and services and are informed that the two companies involved will be jointly collecting or sharing the consumer's information in order to provide the product or service.

We also request that examples be added to clarify the scope of the exceptions contained in the rules. For example, transfers of information between a firm and its registered representative or associated persons should be treated as transfers within a firm and not be viewed as transfers with an unaffiliated third party subject to the rule even if the associated person is an independent contractor. Additionally, transfers necessary to arbitrate a dispute with a customer or to fully investigate a consumer complaint (such as to the former registered representative who is no longer with the firm) should be treated as clearly falling within 248.11(a)(2)(iii).

Finally, we request that an example be added to clarify that the 248.11(a)(2)(ii) exception permits firms to share nonpublic personal information with organizations retained to assist the firm in conducting background and other inquiries. These firms, such as CDC and MIS, perform

a critical function in the securities industry, by consolidating information about an individual's prior dealings in the industry into a readily accessible format. By doing so, they enable securities firms to easily retrieve the information necessary to discharge the firm's know your customer responsibilities. We are concerned that requiring firms to provide consumers an opt-out notice may chill this necessary exchange of information with disastrous effects on many firms' fraud and risk management systems.

## **V. Joint Marketing and Service Agreements**

The joint marketing exception in proposed rule 248.9 recognizes that nonaffiliated companies often join together to provide a better package of services to mutual customers. Provided that each company appropriately protects consumer information in accordance with its privacy policy, the SIA believes that privacy interests are adequately protected.

The SIA requests that the SEC grandfather all joint marketing and servicing agreements executed between firms and their vendors as of November 12, 1999. Many firms currently have agreements in place that require their contracting partner service providers or joint marketer generally to ensure the confidentiality of customer information provided under the agreement. Unless existing agreements are grandfathered, firms would be required to conduct detailed reviews of all service provider or joint marketing agreements currently in force, and (expired agreements, to the extent that vendors may still possess the firm's customer information) to ensure that the agreements require the vendor to treat the consumer information according to the firm's standards. The cost on the industry of both human and financial resources would exceed any relative benefit that could be obtained. Therefore, the SIA respectfully requests that the SEC make clear that the rule is not to have retroactive effect and that existing agreements would be grandfathered. Alternatively, we request that the SEC establish by example that firms may comply with rules concerning existing contractual relationships by sending a notice to all vendors informing them of the G-L-B Act and the rule's requirements, and clearly establishing that the agreement and performance thereunder are governed by such requirements.

The SIA does not believe that the "fully disclose" requirement proposed by the SEC with respect to service providers who fall within rule 248.9 was intended by Congress to apply to service providers. We believe that these disclosure provisions were not initially part of the legislation and were only added with the joint marketing provisions. We therefore respectfully request that the rule make clear that a brief generic disclosure regarding the use of third-party processors and service providers to assist the securities firm as necessary is sufficient. Service providers should be viewed as an extension of the firm performing services that the firm could have otherwise performed itself.

If, however, the final rules as adopted by the SEC require full disclosure of categories of service providers under rule 248.9, the SIA respectfully requests that the SEC clarify and harmonize the interrelationship between rule 248.9 as it applies to service providers and rule 248.10, which addresses certain service providers with respect to which full disclosure is not required. In particular, the SIA requests that the SEC include an example clarifying a firm's

disclosure requirements when the firm engages third parties to assist in preparing communications, documents, mailings, statements, or informational web pages that are related to the servicing of the account relationships but may also be deemed to include the preparation or distribution of marketing or informational material about the company's products or services. In addition, we request that the SEC provide an example under 248.10(a)(3) clarifying that a firm's product or service distributors, such as investment professionals or correspondent brokers who maintain relationships with the ultimate customer of the product or service, are third parties exempted under 248.10 from the firm's opt-out requirements.

Finally, the SIA requests that the SEC clarify that the definition of "joint agreement" set forth in rule 248.9(c) applies only to rule 248.9(b). Without such a clarification, we are concerned that the definition may be applied to rule 248.9(a)(3) and effectively limit the applicability of the exception in rule 248.9 to only arrangements between two financial institutions.

#### **VI. Redislosure and Reuse of Information. - Rule 248.12**

Pursuant to this regulation, financial institutions may from time to time disclose nonpublic personal information about a consumer or customer to a nonaffiliated third party that is itself a financial institution. The SIA believes it is important to emphasize that in those circumstances, the receiving firm is obligated to abide by the restrictions set forth in rule 248.12 to the same extent that it would be if it were not a financial institution and that the consumer or customer does not become a consumer or customer of the second firm simply because of the disclosure of this information.

We request that the SEC include additional examples in proposed rule 248.12 that would address situations where securities firms receive nonpublic personal information from another financial institution. For example, if a bank sells mortgages to a securities firm for purposes of securitization and discloses information to the firm pursuant to rule 248.10(a), the securities firm must comply with rule 248.12 but it need not send privacy and opt-outs notices to the underlying mortgagees. Similarly, if a securities firm provides administrative services for a registered investment adviser and the investment adviser maintains the relationship with the underlying client, the securities firm must comply with rule 248.19(a) but need not send privacy or opt-out notices to the underlying clients.

#### **VII. Prohibition on Disclosing Account Numbers - Rule 248.13**

The G-L-B Act and proposed rule 248.13 broadly prohibit a financial institution from disclosing account numbers and passwords to a nonaffiliated third party for use in telemarketing, direct mail marketing and e-mail marketing. The SIA requests that the SEC clarify that the prohibition under rule 248.13 applies only to disclosing account numbers and passwords to nonaffiliated third parties who are not subject to one of the exceptions under rules 248.9, 248.10, and 248.11. We further request that the SEC clarify that the providing of an account number by a firm to an agent, processor, or service provider for operational support, including support to market products on behalf of the firm, is not prohibited.

The SEC requested comment on whether a consumer should be able to consent to the disclosure of his or her account number. The SIA recognizes the sensitivity of customer account numbers and passwords; however, the SIA urges the SEC to adopt a limited exception for disclosure with customer consent even when the nonaffiliated third party does not fall within rules 248.9, 248.10, and 248.11. For example, disclosure of account numbers may be permitted in the case of two or more companies of a jointly managed service (such as a Internet web-based service where advertising might otherwise be displayed), where the customer consents during the sign-up process to the use of an account number or password as the access code to the jointly managed service for security and convenience purposes. In that example, nonpublic personal information other than account numbers could be disclosed to the other company with the consent of the customer pursuant to rule 248.11(a)(1).

The SEC also invited comment on whether the proposed rule should permit the disclosure of encrypted account numbers if the firm does not provide the marketer the key to decrypt the number. The SIA urges the SEC to revise the rule to specifically permit the sharing of encrypted or truncated numbers.

#### **VIII. Procedures to Safeguard Customer Information and Records - Rule 248.30**

We applaud the SEC for developing a flexible approach to securities firms' information security requirements. The proposed approach is technology neutral and permits firms to develop procedures that best meet their needs, avoiding rigid, proscriptive rules that, given the rapid rate of technological evolution, may do little more than cause firms to adopt procedures that lack the flexibility to adapt to changes in technology and additional risks resulting from such changes.

#### **IX. Effective Date**

The G-L-B Act provides that its privacy provisions shall take effect six months after the date on which the rules implementing the Act's requirements are required to be prescribed, "except . . . to the extent that a later date is specified in the rules prescribed under section 504." The proposed rule contains an effective date of November 13, 2000 (six months after the implementing rules are required to be prescribed). The SIA believes that an effective date of November 13, 2000, would result in the mailing of millions of notices to consumers in December, the peak of the holiday season and a traditionally hectic time for securities firms and consumers alike. Securities firms would be overwhelmed by a burdensome December notice requirement. Moreover, the SEC runs the risk that consumers would not focus on that notice in the midst of the holiday mail deluge.

We respectfully suggest that the SEC consider the November 13, 2000 date as the beginning of a voluntary compliance period. We propose that mandatory compliance would begin no earlier than May 14, 2001, the first business day on which Title II of the G-L-B Act becomes effective. We have proposed May 14, 2001 as the effective date trying to balance the requirements of our member firms with the time table allowed by the G-L-B Act. Nonetheless,



coming into full compliance by May 14, 2001 for some firms will be extremely difficult, and in some cases may not be feasible. For this reason, we request that if the other financial regulatory agencies grant a later effective date, that the SEC do the same. This would not only keep the securities industry on the same footing with rest of the financial services industry, but would establish a uniform effective date across the entire industry for the privacy provisions. This approach would also keep our member firms who have affiliates under the jurisdiction of the other regulators on the same time table. Furthermore, the establishment of a voluntary compliance period would enable firms to use first quarter account statement mailers as a means to satisfy the initial notice requirement. In light of the regulatory and consumer focus on privacy issues, we believe that as a competitive matter, firms will have an incentive to comply fully with the regulation as early as possible.

Additional time is essential because the scope and scale of the required undertaking for firms is unprecedented. Firms will be required to fully implement operational changes necessary to comply on a firm wide basis covering all affiliated entities. For example, the regulations will require significant changes to existing database systems, controls and internal procedures. At a minimum, firms will need to (1) establish and implement new procedures and train associates with regard to the delivery of the notice and customer questions that may ensue; (2) implement new procedures for providing opt-out methods to the customers; (3) hire and train staff for receiving and handling any opt-outs from customers; and (4) evaluate arrangements with nonaffiliated third parties to determine what additional obligations must be imposed. Only after all these procedures have been addressed, will firms have sufficient information to request computer system enhancements, which will take significant lead time, resources and money to implement. Completing these changes in a hasty manner, given the broad scope of the changes, will likely result in mistakes or confusion on the part of the firm, associates and customers alike. In addition, extending the date of mandatory compliance would grant securities firms additional time to conduct detailed audits of their information collection and use practices and would enable firms, perhaps in conjunction with their respective trade associations, to develop more rigorous policies and procedures to safeguard their customer information, consistent with industry standards.

In addition, the preamble discussion indicates that a firm, wishing to disclose nonpublic personal information about an individual who was a consumer as of the effective date, "must provide the notices... and provide a reasonable opportunity to opt out before the effective date." We request that the preamble be revised to more closely conform to the rule clarifying that no privacy or opt-out notices should be required until at least 30 days after the effective date.

For all of these reasons, the SIA respectfully suggests that the SEC use its statutorily granted discretion to extend the effective date of the rules.

## **X. Cost Estimate**

The SIA believes that the costs estimates presented in the proposal vastly understate the costs imposed by the rule. The proposal estimates that the cost of preparing or revising a privacy notice for an investment company or broker-dealer will average 32 hours of professional time

and 8 hours of clerical time, valued at \$4920 and the cost of mailing notices at \$.02 per customer. However, if only one firm, for example, disseminated 15 million notices, the cost would be \$300,000, exclusive of postage. Firms estimate that the cost of the mailing would range from \$0.30 to \$0.49 per mailing. One firm estimates that the per year cost for preparing and mailing the initial and annual privacy notices, and any opt-out notices or interim updates will be \$210,000 -- assuming that the privacy materials could be sent with other regular mailings. Other estimates ranged up to \$18 million.

In addition, the SIA submits that there are other substantial costs that should be considered, including the designing and printing of new notices; modifying account applications and web screens (one estimate for a broker-dealer's web site alone, not including the web sites of affiliated entities, was \$100,000); modifying database, telephony, core processing systems and web-based software to account for receiving and tracking opt-outs; providing the human resources necessary to comply with privacy regulations on a company-wide basis; and addressing the regulatory requirements in contracts and with business partners and service providers. In addition, controls and systems must be designed or altered, implemented and harmonized. The SIA believes that these measures will take substantially more than then 32 hours of professional time that the SEC estimates.

Projecting the total costs of complying with the rule is somewhat difficult at this point because our member firms are still evaluating the requirements of the proposed rule and the implications for operations and systems. The magnitude of the costs will depend somewhat on the final rule that the SEC adopts. For example, the costs of complying with the rules could substantially increase if the SEC adopted very broad definitions of "nonpublic personal information" and "collects." Costs of compliance will also likely be increased if the privacy notice is required to be sent "prior to" the establishment of a customer relationship. Further impact on compliance costs would result if the SEC required firms to adopt policies and procedures to "ensure" that a nonaffiliated third party that receives nonpublic personal information complies with the § 248.12 limits on redisclosure and reuse, and if the grandfathering of joint marketing and service agreements is not permitted. In addition, the costs associated with opt-outs may depend on how the SEC clarifies the opt-out exceptions.

Our membership's best estimates indicate that costs from implementation and compliance with the rule for a large firm could easily total \$1 million, and could possibly run into many millions. One firm even estimates that the charge alone resulting from destroying its old notices would be approximately \$475,000. In short, although exact figures are not yet known, it is clear that the costs of compliance with the rule will be very substantial.

## **XI. Conclusion**

The SIA applauds the SEC for issuing proposed rules that attempt to balance investors' rights to financial privacy with a firm's regulatory and administrative burdens. While we believe the modifications made by the SEC to adapt the G-L-B Act to the securities industry help to make the rules easier to understand and administer, the SIA believes the SEC could go further

Comment Letter of the Securities Industry Association  
Regulation S-P, File No. S 7-6-00  
March 31, 2000  
Page 21

without jeopardizing the objectives of the G-L-B Act. We hope that our comments are useful in fashioning final rules that can be easily understood and effectively administered.

Thank you for the opportunity to comment on the proposed rules. If you have any questions or would like to discuss our comments further, please contact Alan E. Sorcher, Assistant Vice President and Assistant General Counsel at (202) 296-9410.

Sincerely,

A handwritten signature in black ink, appearing to read "Stuart J. Kaswell", with a long, sweeping horizontal stroke extending to the right.

Stuart J. Kaswell  
Senior Vice President and General Counsel